An Arithmetic Technique for Non-Abelian Group Cryptosystem

Abstract

Most public key cryptosystems have been constructed based on abelian groups. It is possible to a cryptosystem based on non-commutative properties of groups. It propose a new public key cryptosystem built on finite non abelian groups in this paper. It is convertible to a scheme in which the encryption and decryption are much faster than other well-known public key cryptosystems.

References


**Index Terms**

Computer Science  
Applied Mathematics
Keywords

Non-Abelian Group, Public key, Encryption, Decryption